AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) Process of securing an access to a data processing server (7) from a client site through at least a first communication network, this server comprising means (8) for handling a protocol of authenticating a client site user, this user being a person, comprising:

- a sequence of receiving and processing identification data of the client site user, ~~and~~

- a sequence of transmitting a voice message (MPA) from the server site to a client site user owned communication equipment through a second communication network, ~~characterized in that this transmitted message (MPA) is a voice message providing to the aforesaid user means for generating an authentication password (MPAUT) intended to be transmitted~~

said communication equipment having a call number that is searched from an authentication data base,

- a sequence of building an authentication password (MPAUT) from said voice message (MPA) directly by said user by applying a key known from said user to the voice message, and

- a sequence of transmitting said authentication password (MPAUT) to ~~the aforesaid~~ said server site through either

~~the~~ said first or ~~the~~ second communication network~~, the call number of the aforesaid communication equipment being searched from an authentication data base~~.

2. (previously presented) Securing process according to claim 1, characterized in that it comprises steps of:

- requesting identification data (ID, MPC) from the client site through the first communication network (4);

- processing the aforesaid data (ID, MPC) and searching an authentication data base (BDA) for a client user owned mobile communication equipment call number;

- calling the aforesaid communication equipment through at least a second communication network;

- after establishing a communication with the aforesaid mobile communication equipment, generating a random or pseudo random password (MPA);

- sending a voice message comprising the aforesaid random password through the second communication network (6);

- requesting the user to provide, from the client site through the first communication network (4) an authentication password (MPAUT) derived from the aforesaid random or pseudo random password (MPA); and

- authenticating the aforesaid authentication password (MPAUT).

3. (canceled)

4. (currently amended) Process according to claim 2 [[3]], characterized in that the authentication password (MPAUT) is built from the random or pseudo random password (MPA) generated by the server and transmitted through the mobile communication equipment, ~~applying a~~ the client user known key ~~that is~~ being embodied within the server authentication data base (BDA), the authentication step comprising a step of converting the aforesaid authentication password into a random or pseudo random authentication password (MPA) by applying the aforesaid key.

5. (previously presented) Process according to claim 1, characterized in that the identification data requested from the client consists of a couple [identification code/client password] (ID/MPC).

6. (previously presented) Process according to claim 1, characterized in that the step of requesting the authentication password (MPAUT) from the user takes place during a predetermined time-out delay beyond which the authentication is denied.

7. (previously presented) Securing process according to claim 1, characterized in that it comprises on the server side the steps of:

- requesting authentication data (ID, MPC) from the client site through the first communication network (4);

- processing the aforesaid data (ID, MPC) and searching an authentication data base (BDA) for a client site user owned mobile communication equipment call number;

- calling the aforesaid communication equipment through at least a second communication network;

- in case the communication is established with the aforesaid mobile communication equipment, send a voice message requesting the user to send an encryption key;

- receiving and recognising the encryption key transmitted by the client by means of the mobile equipment keyboard,

- deciphering by means of the aforesaid encryption key an authentication password (MPAUT) transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and

- authenticating the client password (MPC) which results from the authentication password deciphering.

8. (previously presented) Process according to claim 7, characterized in that the step of receiving the encryption key takes place during a predetermined time-out delay beyond which the authentication is denied.

9. (currently amended) System of securing the access to a data processing server through at least a first communication network, which implements the process according to claim 1, this system comprising at the server site:

- means (8) for handling a protocol of authenticating of a client site user,

- means (2, 8) for receiving and processing identification data of a client site user,

- means (8, 10) for generating and transmitting a message from the server site to a client site user owned communication equipment through a second communication network,

characterized in that ~~this system~~ the message is ~~implemented in order to transmit~~ a voice message, this voice message providing to the aforesaid user means for ~~generating~~ directly building an authentication password (MPAUT) by applying a user known key to the voice message, the authentication password being intended to be transmitted to the aforesaid server site through the first communication network, means (8) being provided for searching from an authentication data base (BDA) the call number of the aforesaid communication equipment.

10. (currently amended) Securing system according to claim 9, further comprising:

- means (8) for searching an authentication data base (BDA), in response to identification data received from an access requesting client site, a client site user owned mobile communication equipment call number;

- means (10) for calling this communication equipment through at least a second communication network;

- means (8) for generating a random or pseudo random password (MPA); and

- means (8) for authenticating an authentication password incoming from the client site, characterized in that the system further comprises:

- means (10, 12) for sending a voice message comprising the aforesaid random password (MPA) through the second communication network, and

- means (2) for requesting the client site user to provide, through the first communication network (4), an authentication password (MPAUT) derived from the aforesaid random or pseudo random password (MPA).

11. (currently amended) Securing system according to claim 9, further comprising:

- means (2) for requesting the client site for identification data (ID, MPC) through a first communication network (4);

- means (8) for processing the aforesaid data (ID, MPC) and for searching an authentication data base (BDA), in response to identification data received from an access requesting client site, a client site user owned mobile communication equipment call number;

- means (10) for calling this communication equipment through at least a second communication network;

- means (10, 12) for sending a voice message which requests the user to send an encryption key;

- means (8) for receiving and recognising the encryption key entered by the user by means of his mobile communication equipment keyboard;

- means (8) for deciphering by means of the aforesaid encryption key an authentication password (MPAUT) transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and

- means (8) for authenticating the client password (MPC) which results from the authentication password deciphering.

12. (previously presented) Application of the securing process according to claim 1 in a system for authenticating

digital creations comprising third parties of time stamping, authentication and archiving connected to a first communication network, characterized in that each third party site locally comprises software means (i) for transmitting securing data in voice form to a client site which requests an authentication operation, through a mobile communication equipment attached to the aforesaid client site and connected to a second communication network, and (ii) for receiving through the first communication network an authentication password resulting from the aforesaid securing data.